

CLAIMS

What we claim is:

1 1. A system for protecting sensitive information residing in server environments,
2 comprising at least one processing device coupled among at least one network and
3 at least one client computer, wherein the at least one processing device:
4 receives at least one electronic transaction query from the at least one client
5 computer via at least one secure channel;
6 evaluates the at least one electronic transaction query for sensitive data;
7 encrypts the sensitive data;
8 transfers the encrypted sensitive data among components of the server
9 environment;
10 receives at least one electronic information query for the encrypted sensitive
11 data from at least one third-party system via the at least one secure channel;
12 decrypts the encrypted sensitive data in response to the at least one electronic
13 information query; and
14 provides the decrypted sensitive data to the at least one third-party system via
15 the at least one secure coupling.

1 2. A method for protecting sensitive information within server environments,
2 comprising:
3 evaluating at least one electronic request received over at least one secure
4 Internet channel; and
5 applying at least one cryptographic operation to sensitive data in response to
6 the at least one electronic request, wherein sensitive data of the at least one
7 electronic request is encrypted before transfer among components of the server
8 environment, wherein encrypted sensitive data of the server environment is
9 decrypted before transfer from the server environment.

1 3. The method of claim 2, further comprising determining that the at least one
2 electronic request includes sensitive data.

1 4. The method of claim 2, wherein evaluating comprises identifying tags
2 indicating that associated data is sensitive data.

1 5. The method of claim 2, further comprising:
2 determining that sensitive data in the electronic request includes at least one
3 user password; and
4 applying at least one hash function to the at least one user password.

1 6. The method of claim 5, wherein the at least one hash function is a keyed hash
2 function or a non-keyed hash function.

1 7. The method of claim 2, further comprising:
2 determining the at least one electronic request includes at least one cookie;
3 applying at least one cryptographic function or checksum to the at least one
4 cookie.

1 8. The method of claim 2, wherein the at least one electronic request comprises
2 at least one protocol over Secure Socket Layer.

1 9. The method of claim 2, wherein the sensitive data comprises at least one data
2 item selected from a group including credit card numbers, credit card information,
3 account numbers, account information, birth dates, social security numbers, user
4 information, and user passwords.

1 10. The method of claim 2, further comprising executing the at least one
2 cryptographic operation using at least one public key.

1 11. The method of claim 2, wherein the at least one cryptographic operation
2 includes at least one operation selected from a group including encryption
3 operations, decryption operations, hash operations, keyed hash operations, and
4 keyed hash verification.

1 12. The method of claim 2, wherein encrypting includes performing at least one
2 operation on the sensitive data selected from a group including hashing and keyed
3 hashing when the sensitive data is a password.

1 13. The method of claim 2, wherein the at least one electronic request comprises
2 at least one encoded key identifier.

1 14. A method for securing sensitive information within server systems, comprising:
2 parsing at least one electronic request received via at least one Internet
3 coupling;
4 determining that the at least one electronic request includes sensitive data;
5 encrypting the sensitive data; and
6 storing the encrypted sensitive data in at least one component of the server
7 system.

1 15. The method of claim 14, further comprising:
2 evaluating at least one request for the encrypted sensitive data, wherein the at
3 least one request is received via at least one coupling with at least one third-party
4 system;
5 decrypting the encrypted sensitive data;

6 providing the decrypted sensitive data to the at least one coupling with at least
7 one third-party system.

1 16. The method of claim 14, wherein encrypting includes performing at least one
2 operation on the sensitive data selected from a group including hashing and keyed
3 hashing when the sensitive data is a password.

1 17. A method for securing sensitive information within server systems, comprising:
2 evaluating at least one electronic request received from at least one third-party
3 system via at least one proprietary channel;
4 determining the at least one electronic request includes a request for
5 encrypted sensitive data and retrieving the encrypted sensitive data;
6 decrypting the encrypted sensitive data; and
7 providing the decrypted sensitive data to the at least one third-party system.

1 18. A system for protecting sensitive information within server systems,
2 comprising at least one processing device coupled among at least one server site
3 and at least one client computer and at least one network, wherein the at least one
4 processing device evaluates at least one electronic request received via the at least
5 one network, wherein the at least one processing device applies at least one
6 cryptographic operation to sensitive data in response to the at least one electronic
7 request, wherein sensitive data of the at least one electronic request is encrypted
8 prior to transfer among components of the at least one server system, wherein
9 encrypted sensitive data of the at least one server system is decrypted prior to
10 transfer among the at least one network.

1 19. The system of claim 18, wherein the at least one processing device
2 determines that the at least one electronic request includes sensitive data by
3 identifying tags indicating that associated data is the sensitive data.

1 20. The system of claim 18, wherein the at least one processing device
2 determines that the at least one electronic request includes sensitive data by
3 identifying tags specified by at least one system administrator that associated data is
4 the sensitive data.

1 21. The system of claim 18, wherein the sensitive data comprises at least one
2 data item selected from a group including credit card numbers, credit card
3 information, account numbers, account information, birth dates, social security
4 numbers, user information, and user passwords.

1 22. The system of claim 18, wherein the at least one cryptographic operation
2 includes at least one operation selected from a group including encryption
3 operations, decryption operations, hash operations, and keyed hash operations.

1 23. A cryptographic appliance for securing sensitive information within a server
2 system, comprising:
3 at least one processing device coupled among at least one server system and
4 at least one Internet coupling to evaluate at least one received electronic request,
5 wherein the at least one processing device;
6 determines when the at least one received electronic request includes
7 sensitive data;
8 encrypts the sensitive data; and
9 transfers the encrypted sensitive data among at least one component of
10 the at least one server system.

1 24. The cryptographic appliance of claim 23, wherein the at least one processing
2 device:

3 evaluates at least one request for the encrypted sensitive data received via at
4 least one coupling with at least one third-party system;
5 decrypts the encrypted sensitive data; and
6 transfers the decrypted sensitive data to the at least one third-party system.

1 25. A cryptographic appliance for securing sensitive information within a server
2 system, comprising:
3 at least one processing device coupled among at least one server system and
4 at least one third-party system, wherein the at least one processing device:
5 receives at least one electronic request for encrypted sensitive
6 information;
7 retrieves the encrypted sensitive information
8 decrypts the encrypted sensitive information; and
9 provides the decrypted sensitive data to the at least one third-party
10 system.

1 26. A computer readable medium containing executable instructions which, when
2 executed in a processing system, protects sensitive information within server
3 environments by:
4 evaluating at least one electronic request received over at least one network
5 coupling; and
6 applying at least one cryptographic operation to sensitive data in response to
7 the at least one electronic request, wherein sensitive data of the at least one
8 electronic request is encrypted prior to transfer among components of the server
9 environments, wherein encrypted sensitive data of the server environments is
10 decrypted prior to transfer among the at least one network coupling.

1 27. An electromagnetic medium containing executable instructions which, when
2 executed in a processing system, protects sensitive information within server
3 environments by:
4 evaluating at least one electronic request received over at least one network
5 coupling; and
6 applying at least one cryptographic operation to sensitive data in response to
7 the at least one electronic request, wherein sensitive data of the at least one
8 electronic request is encrypted prior to transfer among components of the server
9 environments, wherein encrypted sensitive data of the server environments is
10 decrypted prior to transfer among the at least one network coupling.

1 28. A device for protecting sensitive information within server environments,
2 comprising:
3 means for receiving at least one electronic transaction query from the at least
4 one client computer via at least one secure coupling;
5 means for evaluating the at least one electronic transaction query for sensitive
6 data;
7 means for encrypting detected sensitive data;
8 means for transferring the encrypted sensitive data among components of the
9 server environment;
10 means for receiving at least one electronic information query for the encrypted
11 sensitive data from at least one third-party system via the at least one secure
12 coupling;
13 means for decrypting the encrypted sensitive data in response to the at least
14 one electronic information query; and
15 means for transferring the decrypted sensitive data to the at least one third-
16 party system via the at least one secure coupling.